PCT/AU 99/01096

4

Patent Office
Canberra

I, LEANNE MYNOTT, TEAM LEADER EXAMINATION SUPPORT AND SALES hereby certify that annexed is a true copy of the Provisional specification in connection with Application No. PP 7570 for a patent by TELSTRA R & D MANAGEMENT Pty. Ltd. filed on 08 December 1998.

WITNESS my hand this
Second day of February 2000

L. Mynott

LEANNE MYNOTT
TEAM LEADER EXAMINATION
SUPPORT AND SALES

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Regulation 3.2

TELSTRA R&D MANAGEMENT PTY. LTD.

AUSTRALIA

Patents Act 1990

PROVISIONAL SPECIFICATION

for the invention entitled:

"A PUBLIC KEY PROCESS AND A CERTIFICATION METHOD"

The invention is described in the following statement:

A PUBLIC KEY PROCESS AND A CERTIFICATION METHOD

The present invention relates to a public key process and a certification method. The present invention particularly, but not exclusively, relates to public key cryptography and a process for the issuing of digital certificates to bind a person or organisation's identity to a particular public key.

The basis of public key cryptography is the generation of a public and private key pair for use in the encryption and decryption, and signing and verifying, of information transmitted over public access communication lines. Key pairs are mathematically related, but it is not practically feasible to derive a private key from its corresponding public key. A person may openly distribute the public key but the person must keep secret the private key. Anyone wishing to send information to a person encrypts the information using that person's public key. The recipient, being the sole possessor of the corresponding private key, is the only person who can decrypt that information.

For a number of electronic commerce applications, a trusted third party, known as a Certification Authority (CA), is needed to bind a person's identity or information, such as privileges, memberships, account numbers, etc., to their public key. The CA issues a digital certificate, which is essentially a form of electronic identification that binds two or more pieces of information, such as the identity of the person and a particular public key. Throughout the specification a reference to person is intended to include a reference to an organisation or individual.

The process of binding a public key to a person must be secure so that the CA can issue a digital certificate and be accordingly held responsible for it. At present, there is a weakness in a certification process used by CAs where once the CA receives the public key generated by a person's equipment, together with other data concerning the person, a registrar of the CA contacts the person to correctly identify them with reference to the person's data that has been provided. This is normally done by having the contacted person repeat to the registrar personal details, such as mothers' maiden names and drivers' licence numbers. This

identifying information however is only related to the data submitted by the person and does not relate whatsoever to the public key which is used for all future communications. The public key can therefore become separated from the person's data held by the CA or substituted and there is currently no method of relating the public key to the person other than by storing it with the person's personal data. It is desired to overcome this problem or at least provide a useful alternative.

The present invention further provides a certification method, including:

receiving a public key of a public key and private key pair generated by a system of a person to be certified;

processing said public key to generate a communicable code representative of said public key;

forwarding said code to said system for said person;

identifying said person, said identifying including having said person convey said code; and

transmitting a digital certificate, said certificate including said public key.

Advantageously said certificate is able to bind identifying information of said person and said public key.

Preferably said communicable code is a limited character string.

The present invention relates to a process for generating a communicable code from a public key which can be used in an identification process when binding a person's data to the public key.

The present invention also provides a process for forming a communicable code representation of a public key, including:

receiving a public key associated with a person; and

generating said code from said public key.

Preferably the code is generated using a secure one-way hash function.

Preferably the public key is received as a response to an instruction sent to a person to generate a public/private key pair. Preferably the code is sent to the equipment of the person. Preferably the code is communicated during identification of the person. Preferably once the identity of the person is confirmed, a digital certificate is sent to the person.

The present invention further provides an identification process, including:

receiving a public key, as part of a public/private key pair, associated with a person, at an identification body; and

sending a communicable code representation of said public key.

The present invention further provides an identification process, including:

sending a public key, as part of a public/private key pair, associated with a person, to an identification body;

receiving from said body a communicable code representation of said public key.

The present invention also provides a certification system, including:

means for receiving a public key of a public key and private key pair generated by equipment of person to be certified;

means for processing said public key to generate a communicable code representation of said public key;

means for forwarding said code to said equipment for said person; and

means for transmitting a digital certificate when said person is identified by conveying said code, said certificate including said public key.

A preferred embodiment of the present invention is hereinafter described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a block diagram of a preferred embodiment of a certification system; and

Figure 2 is a flowchart of steps executed by the system.

Referring to Figure 1, there is shown a person 20 who can interact with a telephone 42 or the person's computer system 32. The computer system 32 can communicate with the computer system 30 of the CA via a communication channel 60. A registrar of a certification authority 10 interacts with the computer system 30 and a telephone 40 to communicate with and confirm the identity of the person 20. The registrar 10 and the person communicate verbally over a communications channel 62 connecting the telephones 40, 42. The computer systems 30, 32 may communicate with each other independently or on instructions from the registrar 10 or person 20 respectively. The communications channels 60, 62 may be constituted by any voice or data transmission media.

Referring to Figure 2, a person wishing to obtain a certificate from the CA would visit the CA web site 100 using the person's computer system 32. This is the first step in the process of obtaining a certificate and is one way by which the person may perform the second step of filling out the registration form 110 and sending it to the CA over the communications channel 60. The registration form captures personal information about the person which can be used to confirm the identity of that person over the telephone. Once the person fills out and sends the registration form 110, the person is not aware of the subsequent steps in the process until he or she receives a registration ID 210 in the form of an alphanumeric code. The intervening parts 120 to 200 of the process are conducted by the computer systems 30, 32 automatically.

The computer system 30 of the CA receives and processes the registration 120 and sends an instruction to generate the public/private key pair 130 to the computer system 32 of the person. The received registration information may be stored in a database at this point or may be stored once the person's public key is received and the corresponding alphanumeric code is generated together with that information. Once the computer system 32 has received the instruction to generate a public/private key pair, it generates, according to algorithms commonly used by browser applications such as Netscape Navigator or Microsoft Internet Explorer, a public/private key pair 140. The private key is kept securely by the person in the memory of the computer system 32 or another data storage medium, while the public key may be used by anyone wishing to send information to the person. The person's computer system

32 sends the public key 150 to the computer system 30 of the CA. Once the computer system 30 receives the public key it generates a communicable code 180. The public key is represented as a value of the Abstract Syntax Notation No. 1 (described in ASN.1 by ITU) data type SubjectPublicKeyInfo (defined in standard X.509 by ITU), encoded according to the distinguished encoding rules (DER by ITU) and passed through a secure one-way hash algorithm such as SHA-1 (defined in the U.S. Government Federal Information Processing Standard (FIPS) 180-1). The output of the hash algorithm is truncated to 40 bits and converted to 8 base-32 characters. The numerals and upper case letters (excluding '0', '1', 'O' and 'I' to avoid confusion) are used as the base-32 character set. For example, the code may be 8JQ3 UEB5. The code is communicable, to the extent that it is sensibly communicable by the person to the registrar on the communications channel 62, which may include a telephone call or facsimile message. The public key is not sensibly communicable on an identification channel 62 as it is a large mathematical quantity typically consisting of hundreds of decimal digits. The information on the person generated and received is then stored in a database 190 by the CA.

The alphanumeric code is sent to the person as a registration ID 200. The person will probably not know that the registration ID is, in fact, derived from the public key generated by the person's computer system 32. At some time after the person receives the registration ID 210, he or she establishes telephone communication with a registrar of the CA and provides the relevant person identification information 220. The registrar confirms the relevant information 230 and requests the person to say the registration ID 240. Once the person provides the registration ID 250 to the registrar, the CA receives a public key from computer system 30 and a confirmed identity and communicable code from the registrar. The CA compares 260 the code to a value recalculated from the public key using the secure hash algorithm and, if they match, issues a digital certificate that lists the public key and confirmed identity 270. The digital certificate is signed by the CAs private key. The certificate may be sent 280 to the person and stored 290 on their hard drive, floppy disk, smart card, etc. and/or the certificate may be published in another system, such as electronic white pages.

As the alphanumeric code used in the identification process is derived directly from

the public key, the CA can ensure the identification information confirmed by the registrar and the public key are bound as a pair, which ensures the digital certificate contains the correct information.

Modifications and adjustments will be appreciated by a person skilled in the art and may be made to the hereinbefore described invention without departing from the spirit and scope of the invention.

DATED this 8th day of December, 1998

TELSTRA R&D MANAGEMENT PTY. LTD.
By its Patent Attorneys
DAVIES COLLISON CAVE

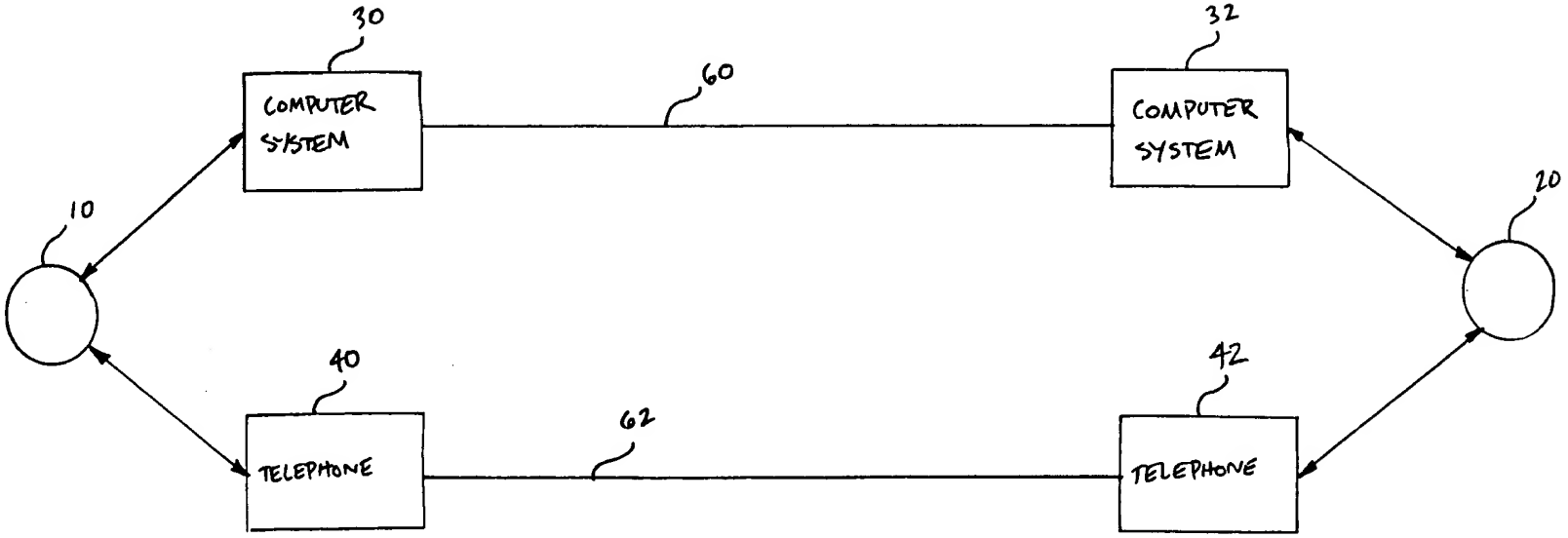
30
COMPUTER SYSTEM
60
32
COMPUTER SYSTEM
10
20
40
TELEPHONE
62
42
TELEPHONE

FIGURE 1

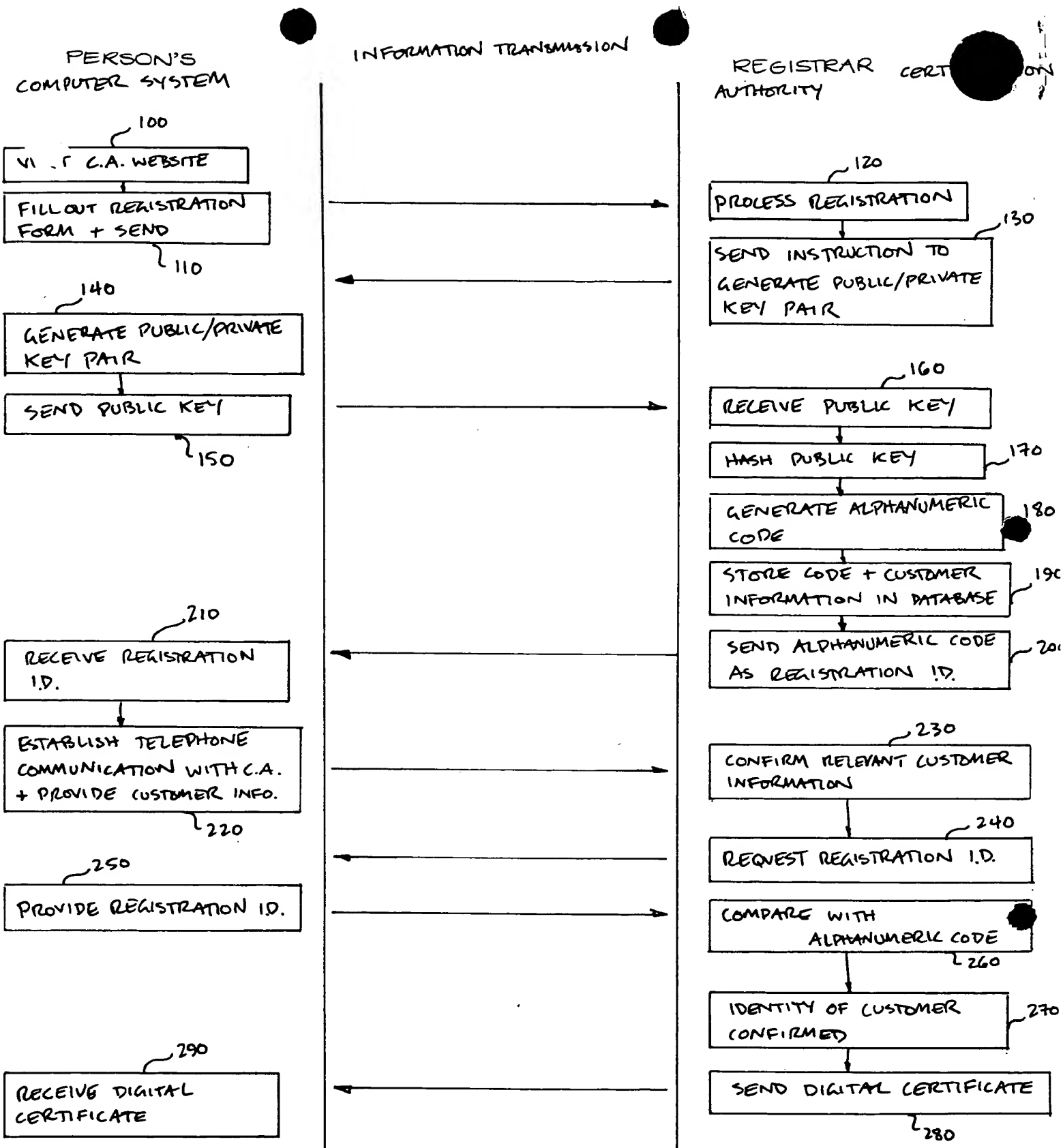
PERSON'S COMPUTER SYSTEM
INFORMATION TRANSMISSION
REGISTRAR CERT ON AUTHORITY
100
VI . T C.A. WEBSITE
FILL OUT REGISTRATION FORM + SEND
110
140
GENERATE PUBLIC/PRIVATE KEY PAIR
SEND PUBLIC KEY
150
120
PROCESS REGISTRATION
130
SEND INSTRUCTION TO GENERATE PUBLIC/PRIVATE KEY PAIR
160
RECEIVE PUBLIC KEY
HASH PUBLIC KEY
170
GENERATE ALPHANUMERIC CODE
180
STORE CODE + CUSTOMER INFORMATION IN DATABASE
SEND ALPHANUMERIC CODE AS REGISTRATION I.D.
210
RECEIVE REGISTRATION I.D.
ESTABLISH TELEPHONE COMMUNICATION WITH C.A. + PROVIDE CUSTOMER INFO.
220
230
CONFIRM RELEVANT CUSTOMER INFORMATION
240
REQUEST REGISTRATION I.D.
250
PROVIDE REGISTRATION I.D.
COMPARE WITH ALPHANUMERIC CODE
260
IDENTITY OF CUSTOMER CONFIRMED
270
290
RECEIVE DIGITAL CERTIFICATE
SEND DIGITAL CERTIFICATE
280

FIGURE 2